

Materials Microcharacterization Collaboratory

<http://tpm.amc.anl.gov/MMC>



Certificate Use for Collaboratories

James A. Rome – ORNL – *jar@ornl.gov*

William E. Johnston – LBNL – *wej@george.lbl.gov*

April 27, 1998

ARGONNE
National Laboratory



NIST

ornl

University of **Illinois**
Urbana-Champaign

What is a collaboratory?



- A new environment that allows convenient, rapid and dynamic interactions to flow unencumbered by the limits of time and distance, *leading to a truly new paradigm in scientific research.*
- Research at a distance.
- A persistent electronic space.

The MMC Environment



- The MMC includes five different resource centers (microscopes + beam lines)
- The user community is distributed through the U.S. and abroad
- Users require high-bandwidth, secure access but may not be able to buy much equipment or software
- Different users require different levels of access (students, researchers, operators).

Cross-platform is required

- From a user survey (~1 year old), almost all users have Macs or PCs. A new survey is in progress and we suspect that more now use PCs.
- A manufacturer survey at the Cleveland microscopy show revealed that they were all switching to Windows NT for microscope control.
- Unix-only solutions will not suffice.

Security and networking

With million-\$ instruments on line, security is a necessity.

- Fast, transparent encryption
- Secure multicast for conferencing and group collaboration
- Accurate and fast knowledge of who is accessing our devices from across the net

Certificates are the key to achieving above

Secure authorization

- For simple applications, strong authentication of the user might suffice.
- But in real life, various stakeholders have control over access to resources and data.
 - ◆ Access can only be allowed after approval by each stakeholder
- The Akenti access control system (William Johnston — LBNL) can solve this need.

<http://www-itg.lbl.gov/security/Akenti/>

The “conventional” approach



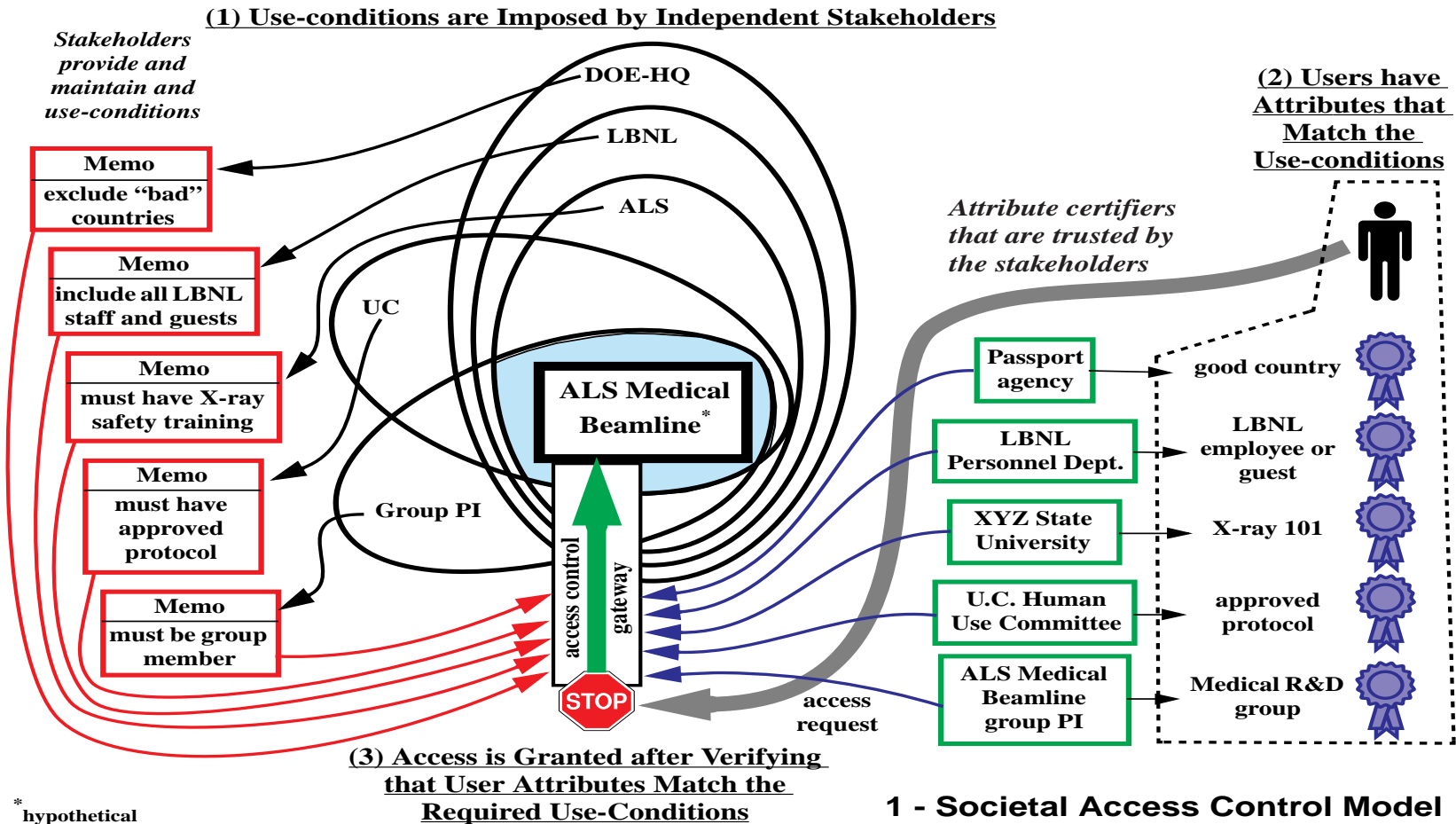
- Stakeholders are identified by (usually) written policy
- Representations of authority (“use conditions”) are made by written, signed procedures, memoranda, etc.
- The required use conditions are satisfied by a set of attributes: organizational membership, training, etc.

The “conventional” approach



- Who and/or what can attest to users' satisfaction of the use-conditions is established by policy: e.g., a token issued by a personnel department, a certificate of training issued by an accredited school, etc.
- Mechanisms are established for checking credentials — an operational authority that compiles a list or rules and validates the users' attributes, etc. (Guard?)

An example of authorization*



1 - Societal Access Control Model

Authorization in “real life”

- Probably, the user is given one document attesting to his satisfaction of requirements. E.g., DOE badge allows entrance to facility.
- The access control enforcer — a door guard, the experiment PI, etc. — validates the capability (e.g., checks the badge) when access is requested.

Akenti implements this model in cyberspace.

Akenti reflects current practice

- Stakeholders independently make assertions about resource use
- Trusted third-parties certify user attributes required for the use conditions
- Authenticated users that possess the required attributes easily gain access

More details available at:

<http://www-itg.lbl.gov/security/Akenti>

An infrastructure is required

- Need dynamic and easily used mechanisms for generation, maintenance, and distribution of the access control information.
- Those that make assertions (e.g., establish the use-conditions or attest to user attributes) must be able to do so within their own working environment.
- Access decisions must be based on assured information and strongly enforced.

Authorization certificates

- Digitally signed documents (an application of public-key cryptography) can provide remote
 - ◆ assured assertions (e.g., enumeration of resource use conditions)
 - ◆ user information (identity and attributes)
- Certification Authorities (CAs) provide identity assurances in the form of widely distributed digitally signed certificates that bind an identity to a public key (analogous, e.g., to a state-issued driver's license)

Authorization certificates



- Signing authorities are the mechanism by which stakeholders generate, sign, and distribute their assertions.
- An access control gateway identifies stakeholder-imposed use conditions and whether a potential user has met these use conditions and controls access to resources (e.g., instruments, communications channels, computing and storage capacity)

Authorization mechanism

- Application-level security services provide secure (confidential and reliable) end-to-end communication and enforce access control decisions (e.g., SSL - the Secure Sockets Layer, and GSS - the IETF's General Security Services API).
- Web browsers (e.g., Netscape) and servers (e.g., Apache), and Certification Authorities and directory servers, can provide a general infrastructure for managing certificates.

Authorization/use certificates

- Allow stakeholders to impose their use conditions in a “natural and convenient” way — by representing them as digitally signed documents that are generated, maintained, and distributed in the stakeholder’s “local” (working) environment.
 - ◆ Passed computer security update training
 - ◆ paid for a session on an on-line facility
 - ◆ human research subject approved

Attribute certificates

- Allow user attribute certifiers to provide user characteristics that match use-conditions, again in a natural and convenient way.
 - ◆ For example, a role certificate can represent many of the user's properties (role-based access control):
 - MMC:** guest, student, researcher, staff
 - Hospital:** orderly, nurse, intern, doctor, specialist, clerk, social worker,....
 - ORNL:** secretary, staff member, section head,....

Identity certificates

- Standard X.509 certificates and Certification Authority infrastructure are used for identifying and authenticating various entities.
 - ◆ Bind user identity (distinguished name, or DN) to user's public key
 - ◆ CN=James A. Rome, UID=jar, OU=Oak Ridge National Laboratory, O=Materials Microcharacterization Collaboratory, L=Oak Ridge, ST=Researcher, C=US

“Akenti” policy engine



- An independent software module that makes access decision by identifying the use-conditions associated with a resource, searches for the corresponding user attributes, and verifies that a potential user matches all stakeholder’s use-conditions.

Capabilities



For a given resource, Akenti provides a

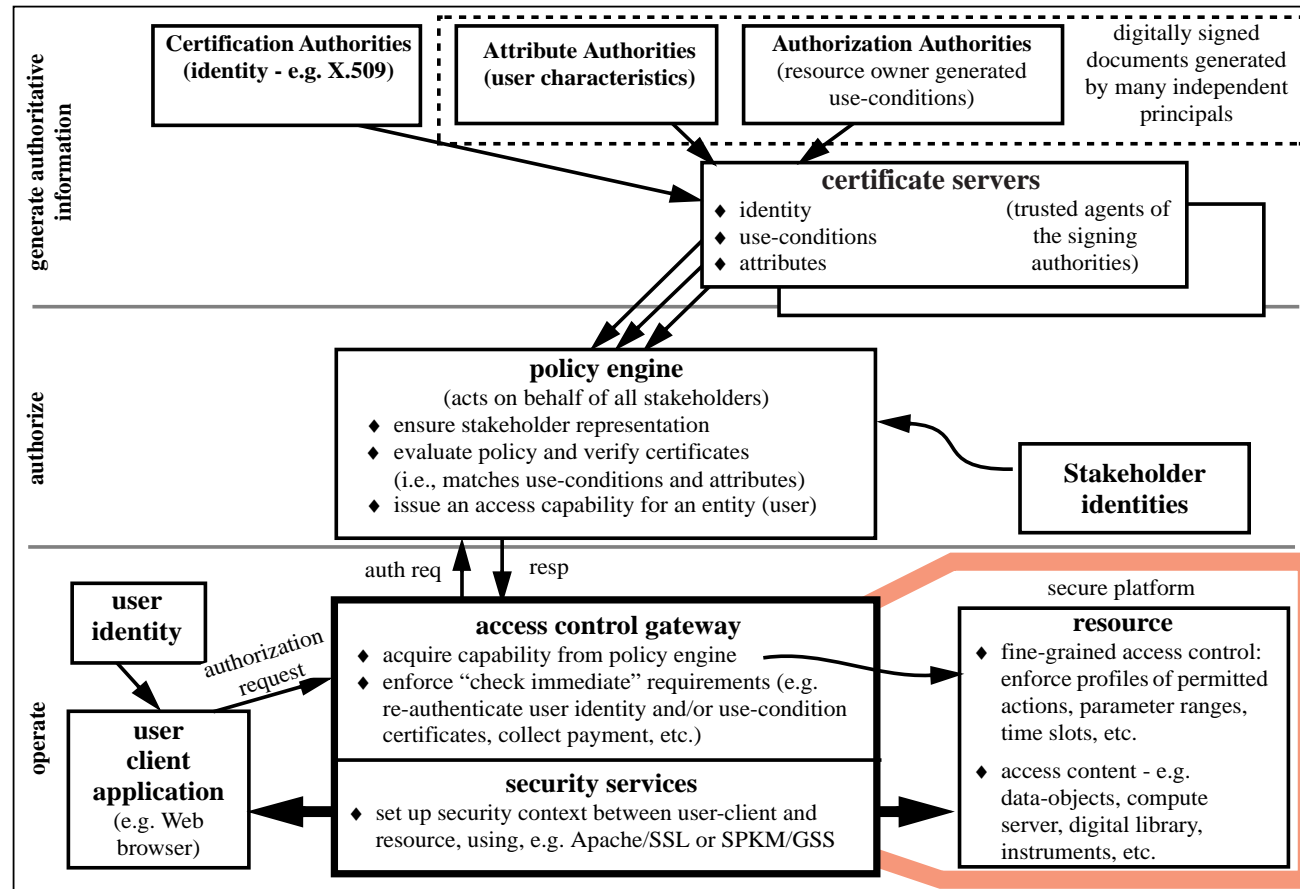
- verified user identity,
- an assured access control decision, and
- a list of permitted actions

to the application (or its agent) that uses these to control specific user actions, and to set up a secure communication channel between the user/client and resource.

Implementation

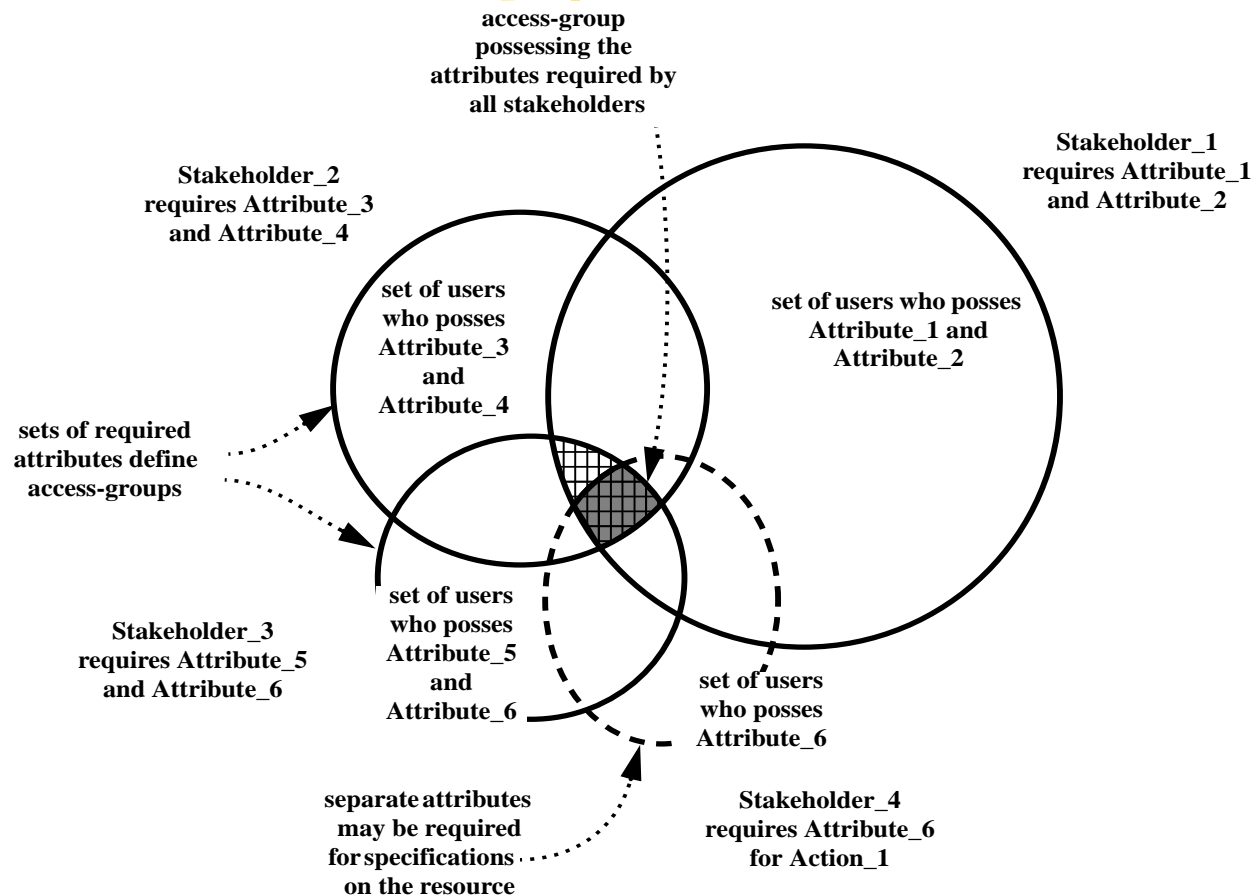
- Java applications provide the mechanism for stakeholders and attribute certifiers to construct use-condition and attribute certificates.
- Any Web server “trusted” by the stakeholders and certifiers can be used to distribute the use-condition and attribute certificates.
- Akenti provides data driven certificate analysis, i.e., no semantic analysis of use-conditions; that is left to the resource server or to out-of-band agreements.

Akenti access control system



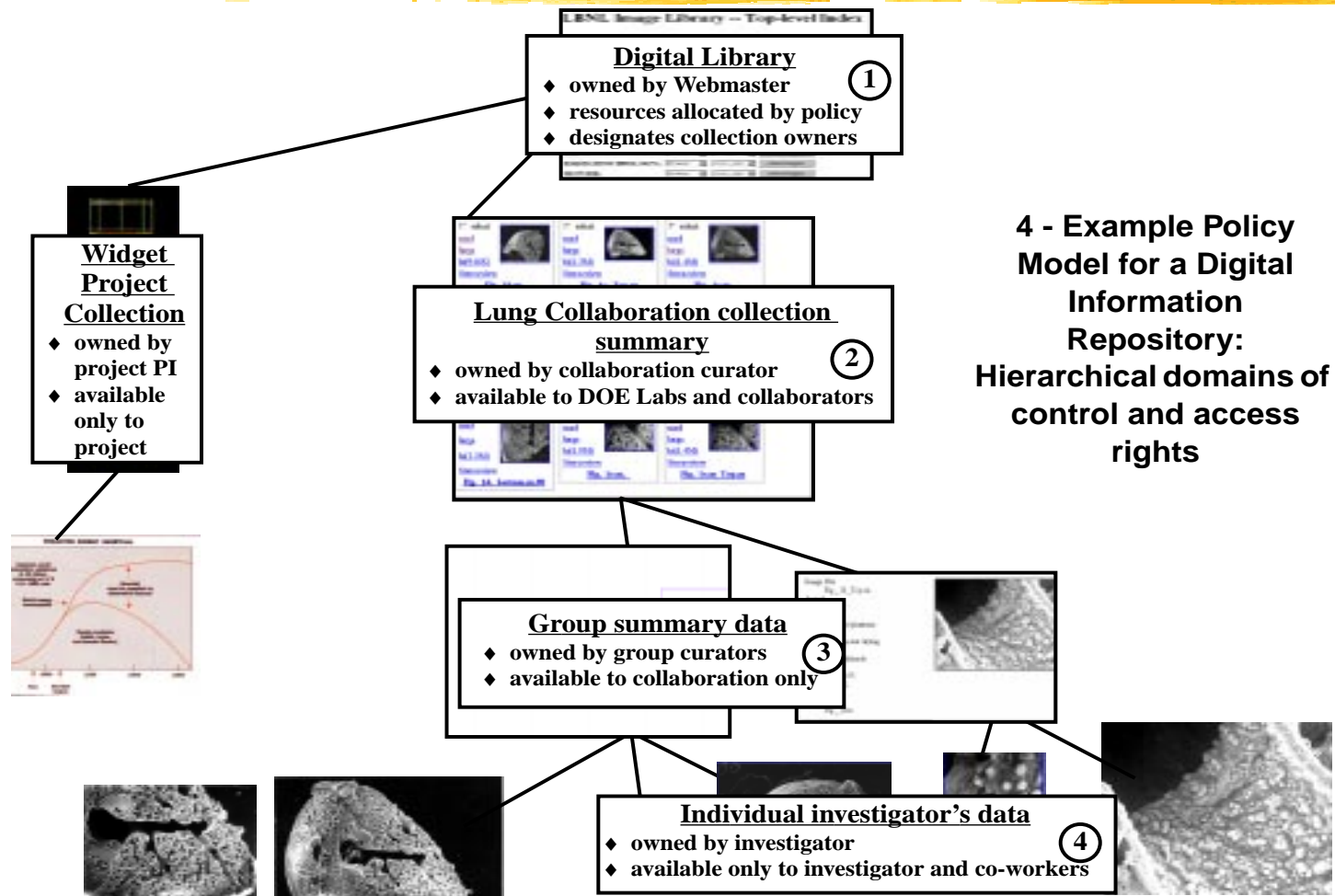
3 - The Overall Architecture of the Authorization Certificate Approach

Access control groups

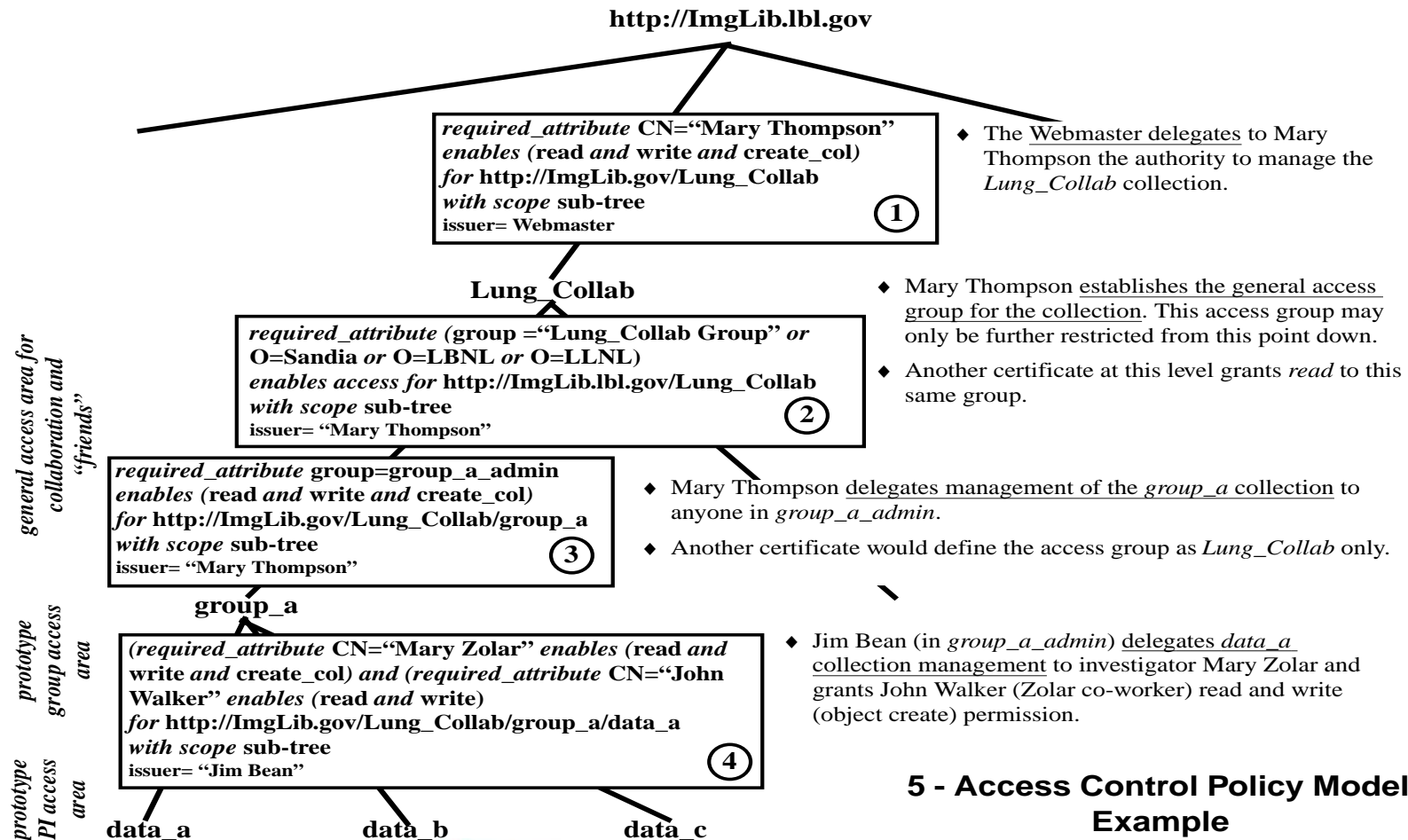


2 - Access Groups are Defined by Several Required Attributes

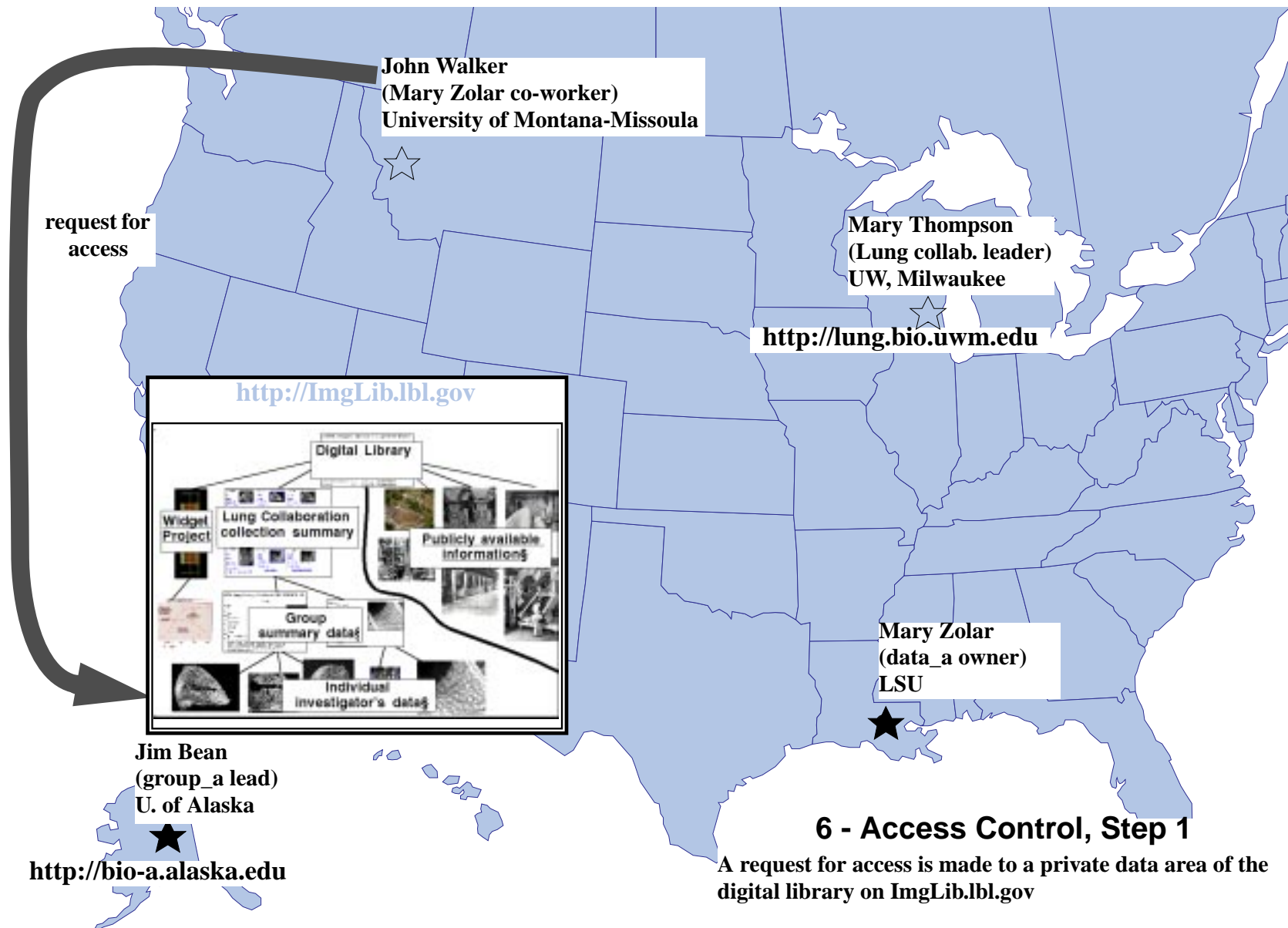
Akenti policy for lung collaboratory

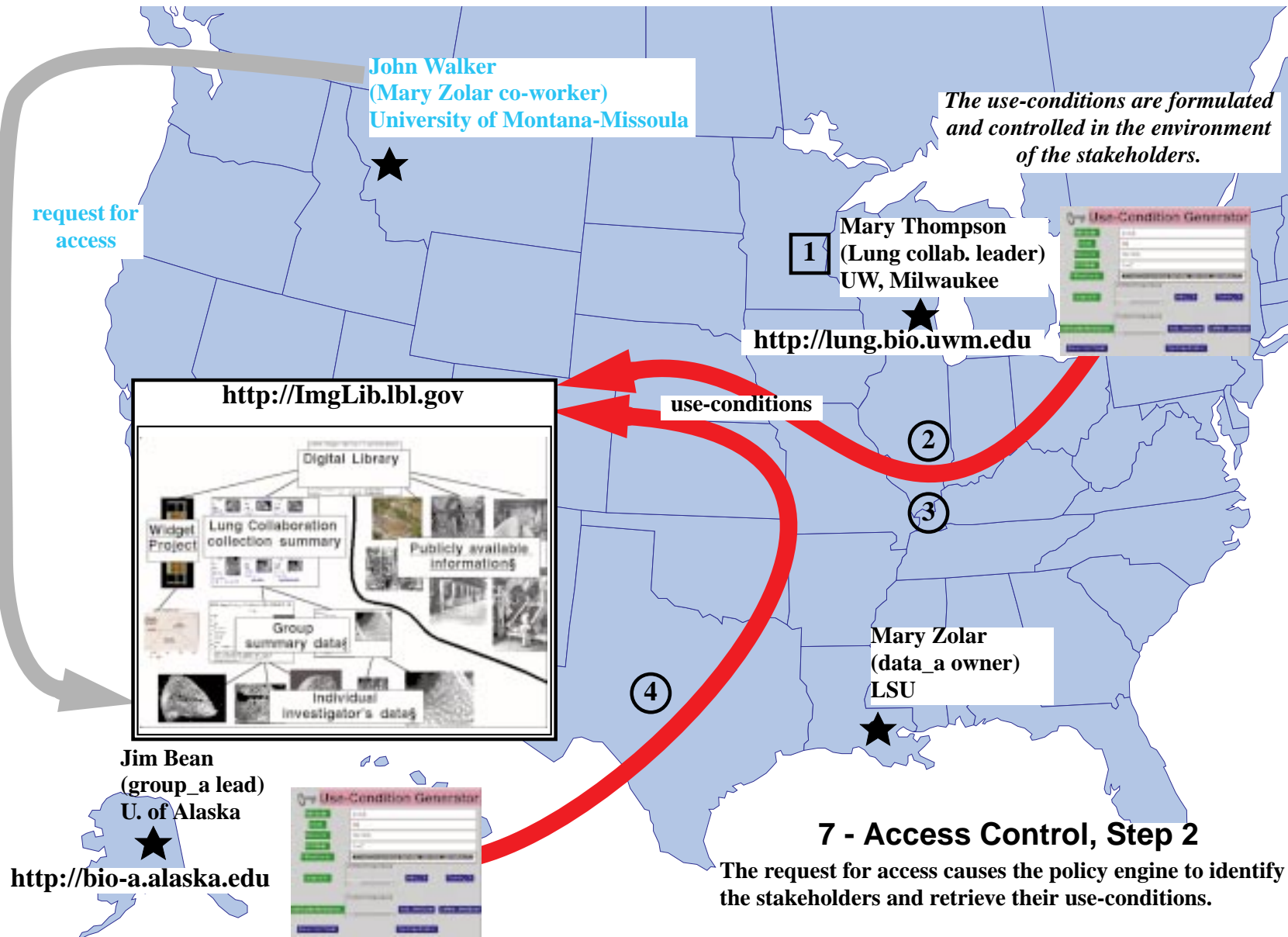


Akenti policy model example

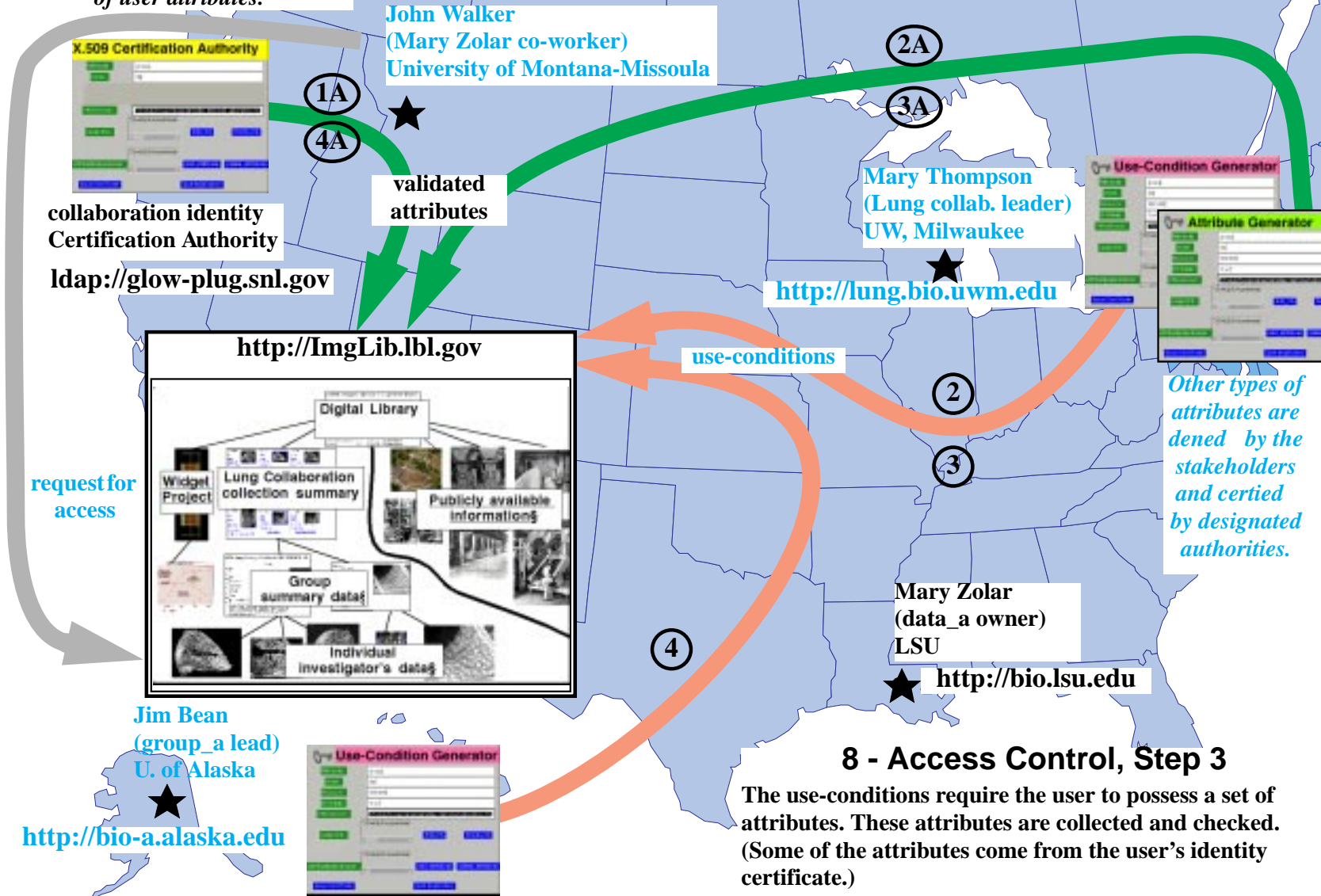


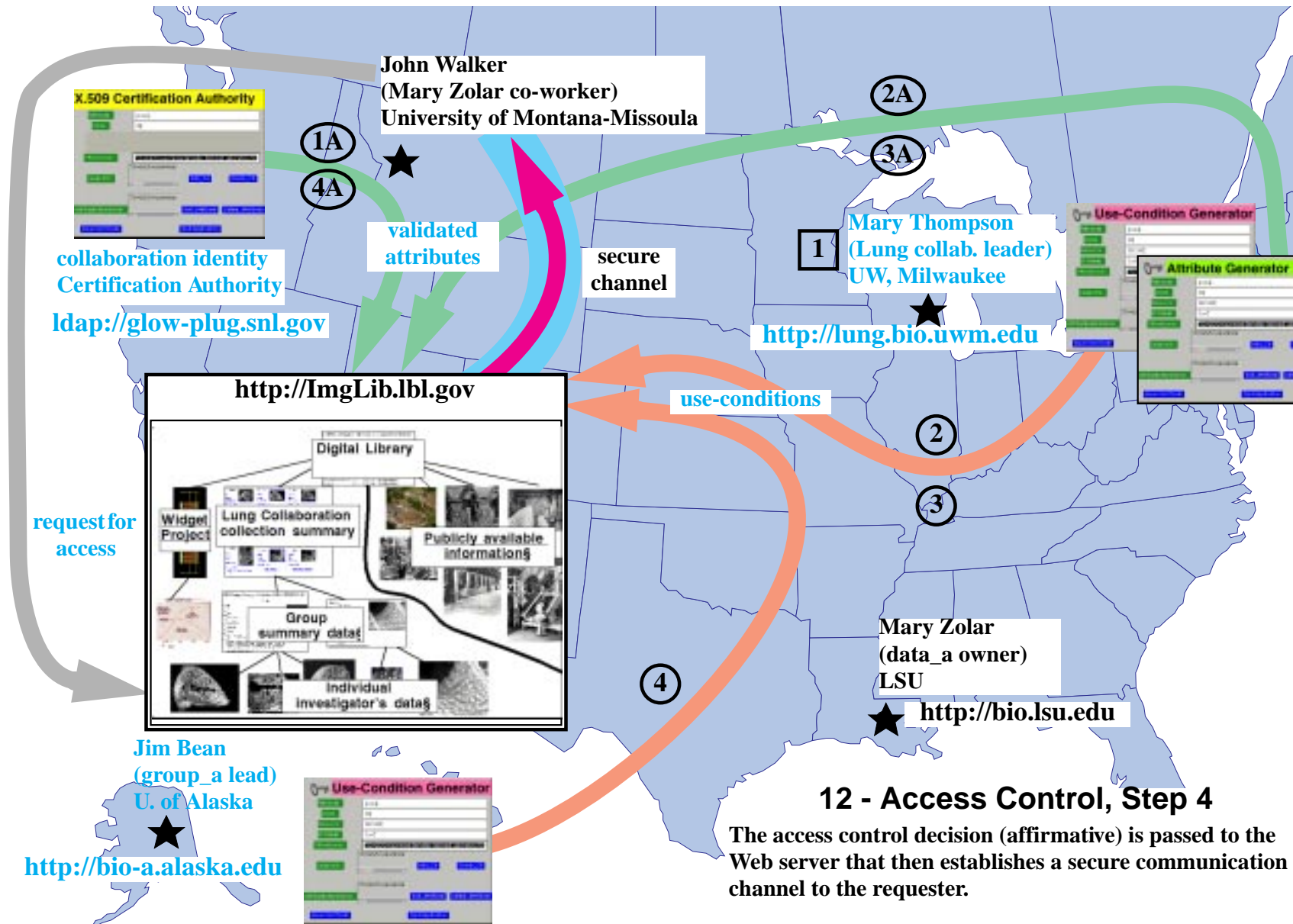
5 - Access Control Policy Model Example





Identity certificates provide one set of user attributes.





Certificate requirements

- Fast access to certificate servers
 - ◆ Certificates must be checked
- Policy engines must check authorization
- Reliability. If the servers are not up, the user is denied access.

There can a significant amount of overhead to set up a circuit for a short transaction.

<http://mmc.epm.ornl.gov/~jar/MMCCerts.html>

Summary



Certificates can be used to express and enforce complicated and flexible security policies.

- X.509 identity certificates
 - User attribute certificate
 - Use-condition certificates
- 
- authorization certificate

Akenti is just now in pilot phase. More details are available from

William (Bill) Johnston [*johnston@george.lbl.gov*](mailto:johnston@george.lbl.gov)